IN THE CLAIMS

Please amend the claims as follows.

1. (Withdrawn) A method of implementing token-based electronic security across multiple secure web sites, in which the user has a security token, comprising:

storing unique token identification information, and the seed value of each token, in a security system;

requiring the user, upon login to a secure web site, to enter at least the code generated by the user's token;

passing the user's token code from the web site to the security system;

using the security system to verify whether or not the user's token code was generated by the user's token; and

passing the verification information from the security system to the web site, for use in web site security.

2. (Withdrawn) The method of claim 1 wherein the requiring step further requires the user to enter a user name and user password.

3. (Withdrawn) The method of claim 2 further comprising the step of:

the web site verifying the user name and user password before passing the user's token code to the security system.

4. (Currently Amended) A method of accomplishing two-factor user authentication, comprising:

providing first and second user authentication methods, wherein the first user authentication method is an authentication method selected from authentication methods based on what a user knows and authentication methods based on a characteristic of the user and the second user authentication ~~methods~~ is based on a token distributed to the user ~~are selected to authenticate at least two factors associated with the user~~;

~~enabling a user to communicate~~ communicating authentication data for both authentication methods to a first web site using the internet;

authenticating the user at the first web site using the first authentication method;

if the user is successfully authenticated at the first web site, enabling the communication of ~~at least some of the~~ token-based authentication data corresponding to the token from the first web site to a second web site using the internet, the authentication data including a token code;

authenticating the user at the second web site based on the token-based authentication data transferred from the first web site ~~using the second authentication method~~;

transmitting results of the authentication at the second web site to the first web site; and

if the authentication at the second web site is unsuccessful, restricting access to sensitive web content on the first web site.

~~wherein both web sites are involved in user authentication using the authentication data and wherein access to content on the first web site is restricted if the user is not authenticated to both web sites.~~

5. (Previously Presented) The method of claim 4, wherein the first web site initially authenticates the user based on the data relating to the first authentication method.

6-7. (Canceled)

8. (Currently Amended) The method of claim [[7]] 4, wherein the first web site communicates to the second web site ~~at least~~ data identifying the user. ~~relating to the second authentication method, and user identification data.~~

9. (Currently Amended) The method of claim 4, wherein ~~one~~ the first user authentication method employs a password.

10. (Canceled)

11. (Currently Amended) The method of claim [[10]] 4, wherein the token is hardware-based, and generates [[a]] the token code ~~that comprises at least some of the data for the authentication method~~.

12. (Original) The method of claim 11, wherein the token is a stand-alone, portable device.

13. (Original) The method of claim 11, wherein the token is USB-based and is accessed by a browser.

14. (Withdrawn) The method of claim 10, wherein the token is software-based, and generates a code that comprises at least some of the data for the authentication method.

15. (Withdrawn) The method of claim 14, wherein the token comprises a browser plug-in.

16. (Original) The method of claim 4, wherein one authentication method employs a fixed complex code.

17. (Currently Amended) The method of claim 16, wherein the fixed complex code comprises a one-time password encrypted using a public key infrastructure.

18. (Original) The method of claim 4, wherein one authentication method is software-based.

19. (Original) The method of claim 4, wherein at least one user authentication method can be used across multiple web sites.

20. (Currently Amended) The method of claim [[10]] 4, wherein the token is embedded in a cell phone.

21-34. (Canceled)

35. (New) A method of strengthening authentication of a user accessing a service web site, wherein the service web site includes a first factor authentication, comprising:

connecting the service web site to a security web site;

configuring the service web site to add a second factor authentication to the first factor authentication, wherein configuring includes adapting the service web site to forward data corresponding to the second factor authentication to the security web site and to receive a authentication result from the security web site;

receiving a service request by the user at the service web site, wherein receiving a service request includes receiving data corresponding to the first authentication factor of the user and data corresponding to the second authentication factor of the user, wherein the second authentication factor is different from the first authentication factor;

authenticating the user using the data corresponding to the first authentication factor at the service web site;

sending a request for the second factor authentication from the service web site to the security web site if the authenticating based on the first authentication factor is successful, wherein sending a request includes transferring the data corresponding to the second authentication factor;

authenticating, in receipt of the request, the user using the data corresponding to the second authentication factor received from the service web site at the security web site;

returning a result of the authentication based on the second authentication factor from the security web site to the service web site; and

determining, at the service web site, whether to authorize the user to access services provided by the service web site according to the result of the authentication returned from the security web site.

36. (New) The method of claim 35, wherein the data corresponding to the first authentication factor is a username and password for the user.

37. (New) The method of claim 35, wherein the data corresponding to the second authentication factor is a token code generated by a security token distributed to the user.

38. (New) The method of claim 37, wherein the security token is a software-based token.

39. (New) The method of claim 35, wherein sending a request for the second factor authentication further includes checking, at the service web site, whether the second factor authentication is requested by the user.

40. (New) The method of claim 35, wherein sending a request for the second factor authentication further includes transferring the data corresponding to the first authentication factor.

41. (New) The method of claim 35, wherein authenticating the user using the second authentication factor at the security web site includes validating information in the request for the second factor authentication received from the service web site.

42. (New) A system for strengthening authentication of a user requesting one or more services, comprising:

a plurality of service web sites, wherein the service web sites provide services accessible by the user, wherein each service web site includes a first authentication module installed thereon, wherein the first authentication module is configured to:

receive, from the user, a service request, wherein the service request includes data corresponding to a first authentication factor of the user and data corresponding to a second authentication factor of the user, wherein the second authentication factor is different from the first authentication factor; and

authenticate the user using the data corresponding to the first authentication factor; and

a security web site operatively coupled with the plurality of service web sites, wherein the security web site includes a second authentication module installed thereon, wherein the second authentication module is configured to:

receive a request for second factor authentication of the user from one of the service web sites, wherein the request includes the data corresponding to the second authentication factor of the user;

authenticate, in receipt of the request, the user using the data corresponding to the second authentication factor received from the service web site; and

return a result of the authentication based on the second authentication factor to the requesting service web site.

43. (New) The system of claim 42, wherein the data corresponding to the first authentication factor is a username and password for the user.

44. (New) The system of claim 42, wherein the data corresponding to the second authentication factor is a token code generated by a security token distributed to the user.

45. (New) The system of claim 44, wherein the security token is a software-based token.

46. (New) The system of claim 42, wherein the first authentication module is further configured to check whether the second factor authentication is requested by the user.

47. (New) The system of claim 42, wherein the first authentication module is further configured to transfer the data corresponding to the first authentication factor to the security web site.

48. (New) The system of claim 42, wherein the second authentication module is further configured to validate information in the request for the second factor authentication received from the service web site.

49. (New) A method of adding a second factor of authentication to a first web site having a first factor of authentication, the method including:

distributing a token to a user;

providing a second website to authorize the user based on the token;

receiving authorization data at the second web site from the first website, the authorization data including user identification data as a function of the first web site successfully authorizing the user;

authorizing the user at the second web site based on the token and the user identification data; and

if the authorization at the second website is successful, transmitting data to the first web site indicating the user has been successfully authenticated using at least two factors of authentication, wherein the user is granted access to web content on the first web site only if the user has been authenticated using at least two factors of authentication.

50. (New) A method of adding a second factor of authentication to a plurality of web sites having a first factor of authentication, the method including:

distributing a token to a user;

providing an authentication web site to authorize the user based on the token;

receiving authorization data from a first web site from the plurality of web sites, the authorization data including user identification data as a function of the first web site successfully authorizing the user;

authorizing the user at the authentication web site based on the token and the user identification data; and

if the authorization at the authorization website is successful, transmitting data to the first web site indicating the user has been successfully authenticated using at least two factors of authentication, wherein the user is granted access to web content on the plurality of web sites only if the user has been authenticated using at least two factors of authentication.